LA-UR-15-22642
Approved for public release; distribution is unlimited.

Title: Insider Threat Case Studies at Radiological and Nuclear Facilities

Author(s): Pope, Noah Gale
Hobbs, Christopher

Intended for: IAEA National Training Course

Issued: 2015-04-13

Insider Threat Case Studies at Radiological and Nuclear Facilities

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Insider Threat Case Study:

Theft of HEU at the Luch Scientific Production Association, Podolsk, Russia

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Research Methodology

- Case studies provide a very good source to illustrate that malicious acts by insiders have occurred.
- Throughout the course I will present case studies that are based on independent research from outside the IAEA
- This case study was derived purely from open sources including peer-reviewed academic articles, news reports and government testimony and statements by subject matter experts (SMEs):
  - Minor variations in different accounts, reconciled as much as possible

- Wider contextual information on the nuclear security situation in FSU in the early 1990s has also been included

Overview

- **Facility:** Luch Scientific Production Association, Podolsk (40km South West of Moscow), Russia
- **Date:** Late-May to early-September 1992
- **Incident:** Theft of weapons-grade highly enriched uranium (HEU) – 90% ^{235}U
- **Perpetrator:** Leonid Smirnov, Luch Scientific Production Association
- **Impact:** Approximately 1.5 kg was stolen and later recovered (first documented theft of HEU from a nuclear facility in the FSU)

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Profile – Leonid Smirnov

- Had worked at Luch Scientific Production Association for over 25 years:
  - Chemical engineer working on nuclear reactors for Soviet space programme
  - Major role: Dispense HEU to research teams

- Intended to sell HEU for financial gain, 'to buy a new stove and refrigerator':
  - Does not appear to have had a buyer in mind, planned to sell to firms in Moscow, thought he'd have 'no trouble selling it'

Incident timeline

- Early 1990s dissolution of Soviet Union:
  - Reduction in working conditions, wages for nuclear FSU scientists & hyper inflation => Financial hardship
- Smirnov apparently became aware of the potential value of HEU via reading an article in a Russian news paper article:
  - "I read an article on someone stealing 1200 grams of uranium… The idea flashed through my mind… why can't I do the same? "

Incident timeline

- May 1992 – He started removing small quantities (25-70 grams) of HEU as UO_2 powder, while his colleagues were out of the room:
  - Siphoned off ~1% of the 3% 'irretrievable loss'
  - 20 to 25 diversions over a 5 month period
- Stored the HEU at his home on his balcony in a lead container

Incident timeline

- 9th October 1992 arrested at Podolsk Railroad Terminal with most of the HEU concealed in three lead cylinders within a briefcase:
  - Apprehended purely by chance, having bumped into neighbours being followed by police for stealing batteries from their factory
  - Was planning to travel to Moscow to sell the HEU
- March 1993 - Tried, found guilty of stealing and storing nuclear material and sentenced to three years probation

Security system failures

- What were the weaknesses in the security system at Luch that enabled Smirnov to steal the HEU?

Security system failures

- Weak nuclear material accounting and control (NMAC):
  - Process allowed for a 3% 'irretrievable loss'
  - Missing 1.5 kg didn't show in balance books
  - Not a weakness unique to Luch:
    - In 1992 employees of Chepetsk Mechanical Plant in Glazov, Russia exploited 4% allowed inventory loss to diverted LEU
- No remote visual surveillance or 'two-person' rule
- No nuclear material detection system:
  - No detection devices (e.g. portal monitors) at facility doors, checkpoints etc.
  - No bag searching upon entrance and exit

References

- Zaitseva, Lyudmila and Kevin Hand, 'Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users, *American Behavioral Scientist'* Vol. 46, No. 6, p. 825 (2003)
- Potter, William C. (1996), 'Nuclear Leakage from the Post-Soviet Nuclear States,' Oral Presentation before the Permanent Subcommittee on Investigations US Senate Committee on Governmental Affairs, available viahttp://www.bu.edu/globalbeat/pubs/papers/w_potter.html (13th March 1996)
- Sam Roe, 'Trafficking in stolen nuclear material on the rise', Chicago Tribune,http://articles.chicagotribune.com/2002-01-31/news/0201310215_1_nuclear-materials-nuclear-device-nuclear-weapon (31st January 2002)
- Transcript of interview with Leonid Smirnov, Public Broadcasting Service, http://www.pbs.org/wgbh/pages/frontline/shows/nukes/stuff/script.html (November 1996)

Insider Threat Case Study:

Theft of UO_2 at GE Low Enrichment Uranium Plant, Wilmington, United States

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Methodology

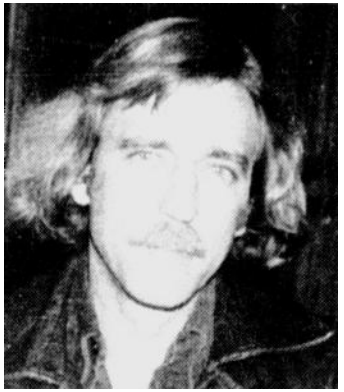
- This case study drew largely on US Nuclear Regulatory Commission reports into the incident, supplemented by news reports
- The information obtained was very consistent across the different sources

Overview

- **Facility:** GE Nuclear Power Plant in Wilmington, North Carolina, United States
- **Date:** 26th January 1979
- **Incident:** Theft of UO_2 powder (LEU)
- **Perpetrator:** David Learned Dale, temporary employee of a GE subcontractor
- **Impact:** Nuclear material successfully diverted without detection, later recovered following a failed blackmail attempt and returned

Profile – David Learned Dale

- Employed as a chemical technician by a GE subcontractor (temporary position)
- Motive unclear:
  - Threatened to send uranium to newspapers & anti-nuclear groups
  - Dale told the FBI it was to obtain money to take his girlfriend out to dinner
  - His brother testified that David had become depressed two weeks before the incident as his job at GE was due to expire in the next few months
- Primitive blackmail attempt:
  - Letter written in his own hand
  - Had no plan for obtaining the ransom money



KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Incident timeline

- 26th January 1979, 10:50pm – Dale entered the plant with the night shift (having already worked the day shift)
- Penetrated the security system:
  - Showed his Florida driving license (same colour as permanent staff badge) to access to a restricted area
  - Drove through a temporarily removed fence & parked his car adjacent next to the building where he worked which contained the UO_2

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Incident timeline

- Using his own key card he entered the Chem Tech Lab where he donned protective clothing and picked up a two wheeled cart and a container used to ship chemicals

- He then proceeded to the nearby uranium store via a door, which although normally locked was ajar due to a mechanism malfunction

Incident timeline

- Once there he removed two 5-gallon cans of UO_2 which he placed in his shipping container and transported back to the Chem Tech Lab
- Back in the lab he opened one of the cans and removed some of the UO_2 (for later use in his blackmail scheme)
- Using the two wheeled cart he then transported the remaining material back to his car and loaded it into the boot, before leaving the plant the same way he entered just before midnight

Incident timeline

- 29th January 1979 - Plant manager, Randall J. Alkema arrived at work to find a letter and a sample of UO_2 powder at his door:
  - Letter demanded $100,000 for the return of two GE 5-gallon containers of UO_2
  - Claimed that material had been removed from the drums & would be sent to newspaper editors, senators, anti-nuclear groups and others if demands were not met
  - Threatened to disperse nuclear material through a large city
- Authenticity of claim verified based on serial numbers provided by Dale, FBI contacted and investigation launched

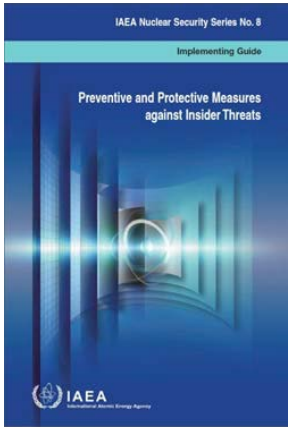
Incident timeline

- 1st February 1979:
  - Dale was arrested by the FBI
  - UO_2 recovered in a field 5 miles from the plant

- Incident is alleged to have cost GE $1 million dollars, due to the plant being closed while searching for the missing uranium

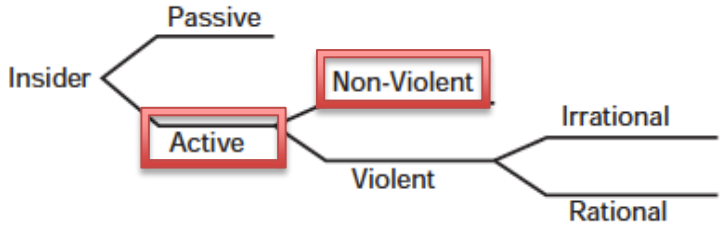
Insider attributes

- Would you categorise Dale as:
  - Active vs. Passive?
  - Violent vs. non-violent?



- How would you assess Dale's level (low, medium, high) of:
  - Access?
  - Authority?
  - Knowledge?

Insider attributes - Dale



- Access: **MEDIUM**
  - Doesn't appear to have had access to the uranium store, but access to an adjacent lab and equipment needed to safely handle and move the nuclear material
- Authority: **LOW**:
  - But didn't need the support of anyone else
- Knowledge: **HIGH**:
  - Had tested security systems for vulnerabilities:
    - Previously gained access with his drivers license
  - Opportunistically took advantage of temporarily removed fence
  - Understood that the 5-gallon cans would be too heavy to carry without the right equipment

Security system failures

- What were the weaknesses in the security system at Wilmington that enable Dale to steal LEU?

Security system failures

- Weak access control system:
  - Dale was able to gain access with the night shift on the 26th of January by showing his Florida driver's license, same blue background colour as GE badge (contractor badges were yellow)
  - Accessed nuclear material through a door that was normally locked (no mitigating measures in place)

- Weak physical protection system:
  - Gate/fence had been temporarily removed, no additional protection measures to limited vehicle access had been enacted

Major sources

- E. Morris Howard, 'Attempted Extortion – Low Enriched Uranium', NRC Information Notice No. 79-02, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1979/in79002.html (2nd February 1979)
- E. Morris Howard, 'Attempted Extortion – Low Enriched Uranium', NRC IE Circular No. 79-08, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/circulars/1979/cr79008.html (2nd February 1979)
- "Dale gets 15 years for uranium plot", *Wilmington Morning Star*, 9th May 1979

In popular culture

THE URANIUM THIEF (Evan)

Written and Directed by: Joel Coen & Ethan Coen

CAST

David Learned Dale - Tim Blake Nelson

Melinda Dale - Marisa Tomei

NERT Commander Stiles - Chris O'Dowd

Garrett Dale - Alex Watson

Bonnie Smith - Debby Ryan

Lynn Smith - Frances McDormand

Harry Smith - Kevin Pollak

Tagline: Hunger can make a thief of any man.

Source: http://baitanoscarnominations.weebly.com/the-uranium-thief.html

Insider Threat Case Study:

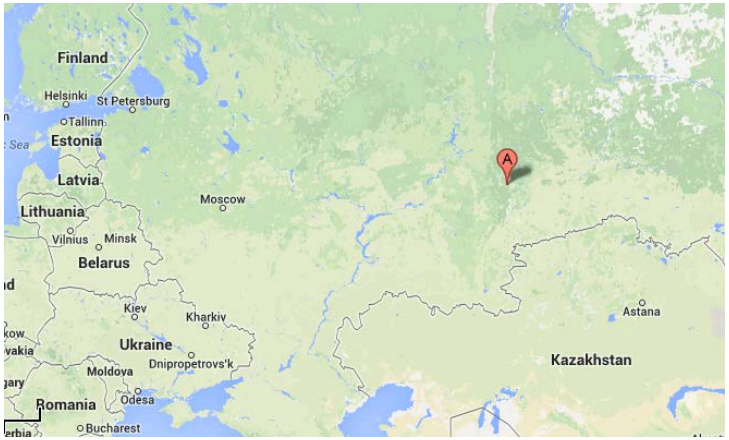
Stable Isotope Diversion at Elektrokhimpribor, Russia

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Overview

- **Facility:** Elektrokhimpribor (Electrochemical Instrument Building Combine; AKA Elektropribor), Lesnoy, Russia
- **Incident:** Theft of rare isotopes, ^{203}Tl, ^{87}Rb and ^{168}Yb (used for medical and industrial purposes) in the early 1990s
- **Perpetrators:** Multiple cooperative insiders
- **Impact:** Loss of revenue estimates vary from several million dollars to $500 million; jail terms of 3 to 5 years for the individuals involved; damage of Elektrokhimpribor's international reputation



KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Profile – Multiple colluding insiders

- Financial motivation (collapse of USSR):
  - Russian companies struggled to efficiently export stable radioisotopes => significant reduction in pay
- Nine(?) employees of Elektrokhimpribor, other reports mentioned only six insiders:
  - Kascheyev, Director of Stable Isotope Production
  - Yaroslavtsev, Deputy Director of Stable Isotope Production
  - Tunin, Head of the plant's technical section
  - Tuinov, Konoplina, Usoltsev, Dubininher, Chernousov; - a mix of engineers, chemists and technicians
  - Korolev, Deputy Head of Finance

Incident timeline

- Kascheyev, Director of Stable Isotope Production at Elektrokhimpribor devised a scheme to divert isotopes from legitimate production processes:
  - Diverted 5-10% of isotope solution, before diluting with distilled water to avoid detection
  - Isotopes were then extracted from the diverted solution using experimental equipment that was being tested at the facility
  - Diverted isotopes then sealed in tubes and removed from the facility

Incident timeline

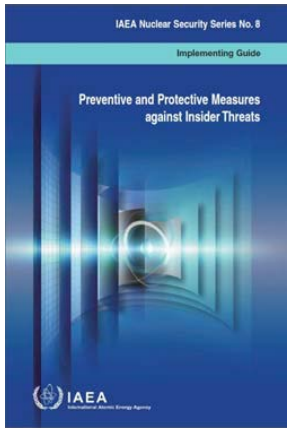
- The diverted isotopes were then purchased by Alexander Podkidyshev, Director of the Russian State Center for Stable Isotopes, at well below market prices, before he resold them to his own company for a large profit:
  - The isotopes where then exported from Russia via Stabis, a Russian isotope export company, also headed by Podkidyshev
- Police alerted and investigation launched, due extravagant displays of wealth (cars and houses) by Elektrokhimpribor employees:
  - Out of place in Lesnoy, where Elektrokhimpribor (the main source of employment) was known to pay small salaries

Incident timeline

- April 1993, individuals arrested but denied they had done anything wrong:
  - Claiming that they had used waste materials and a method he has invented for isotope purification and they had exported the isotopes through a state-sanctioned export company
  - Saw their actions as a ‘way out of poverty’
- May 2000, individuals involved were found guilty of misappropriation:
  - Sentenced to three years, but due to time already served in custody were released immediately (except Podkidyshev who was given an additional 2 year term)

Insider attributes

- Would you categorise Elektrokhimpribor insiders' as:
  - Active vs. Passive?
  - Violent vs. non-violent?

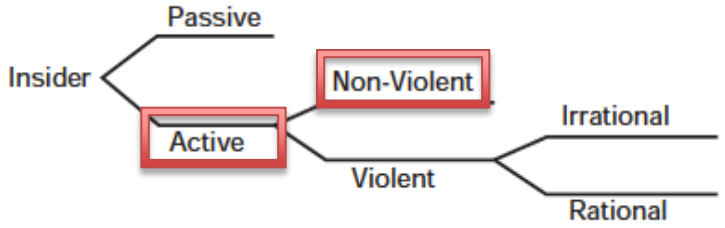


- How would you assess Elektrokhimpribor insiders' level (low, medium, high) of:
  - Access?
  - Authority?
  - Knowledge?

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Insider attributes - Elektrokhimpribor



- Access: **HIGH**
  - Scientists and technicians with hands on access
- Authority: **HIGH**:
  - Director of Elektrokhimpribor was involved
- Knowledge: **HIGH**:
  - Detailed (and innovative) technical knowledge of the production process
  - Understanding of export process; located a buyer

Security system failures

- What were the weaknesses in the security system that enabled stable isotopes to be stolen?

Security system failures

- Bypassed Nuclear Material Accounting and Control (NMAC):
  - Accounting audits provided no evidence of diversion:
    - No processes to detect dilution of isotope solution
  - Colluding insiders at every stage of the production and export process
- Weak nuclear security culture:
  - Others at the plant failed to report the illicit activities, justifying their colleagues actions because ‘there was no other way… to make money’
- Lax law enforcement => No real deterrent:
  - Minimal punishment: jail time only that served while awaiting trial; returned to work at the same facility (albeit without security clearances & positions of authority)

References

- 'Appendix I: Case Studies', in Igor Khripunov and Nikolay Ischenko (Eds), *Proceedings of the NATO Advanced Research Workshop on Nuclear Security Culture: From National Best Practices to International Standards Moscow, Russia 24–25 October 2005*, IOS Press (2007)
- 'Court verdict in the isotope theft case in Lesnoy', Nuclear Threat Initiative, http://www.nti.org/analysis/articles/court-verdict-isotope-theft-case-lesnoy/ (30th June 2000)
- Zaitseva, Lyudmila and Kevin Hand, 'Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users, *American Behavioral Scientist'* Vol. 46, No. 6, p. 826 (2003)
- 'Reducing Nuclear and Biological Threats at the Source', US Subcommittee Hearing, 22nd June 2006, http://purl.access.gpo.gov/GPO/LPS81015

Insider Threat Case Studies:

Sabotage at Koeberg Nuclear Power Plant, South Africa

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Overview

- **Facility:** Koeberg Nuclear Power Plant, South Africa
- **Date:** 18th December 1982
- **Incident:** Sabotage attack
- **Perpetrator:** Rodney Lawrence Wilkinson, a temporary employee at Koeberg, initially worked at Koeberg for 18 months, then later rehired
- **Impact:** Damage estimated at R500 million (~$50 million), delayed commissioning of plant by 18 months; no casualties or radiation release (nuclear fuel in storage waiting for loading)

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Profile – Rodney Wilkinson

- University dropout (had studied 'Building Science and Politics'), living in a commune in Cape Town, a former South African National Fencing Champion but with a shady past:
  - Went AWOL while doing national service during South African intervention in Angolan civil war
  - Anti-nuclear campaigner
- Hired as a safety officer (2nd period of employment):
  - Had previous accessed a forbidden area & taken (and drunk!) alcohol onsite (bottle of vodka) – reprimanded by guard but no further action

Rodney Wilkinson , March 2015

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Incident timeline

- Early-1980s: Wilkinson started work at Koeberg
- After ~ 18 months of employment he stole site plans & smuggled them to Zimbabwe to meet with ANC members (encouraged by his girlfriend):
  - Vetted by ANC, plans authenticated and bombing Koeberg was discussed (Operation Mac)
  - Decided that Wilkinson would carry out the attack

Incident timelines

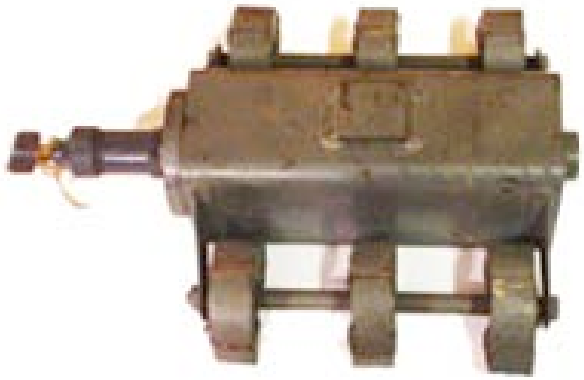
- Planned attack with ANC guerilla leader in Swaziland (re-hired by Koeberg):
  - Wilkinson visited Swaziland once a month (vacation pretext)
  - Identified a strategy (maximise embarrassment for authorities, minimise loss of life) & selected four targets (two reactor heads; containment building; control room)

Incident timeline

- Attack set for the 16th December 1982, a significant date:
  - Anniversary of the Battle of Blood River, Boers defeated the Zulu's
  - Anniversary of foundation of Umkhonto weSizwe (ANC guerilla army), known as MK Day
  - This date had been identified by the authorities as a likely attack date

Incident timeline

- Wilkinson and his girlfriend acquired four limpet mines from an ANC arms cache in the Karoo
- Smuggled into Koeberg one by one in wine decanters via a hidden compartment in Wilkinson's car & then stored in his desk drawer
- Then carried into the reactor building under his overalls, through a security gate



Typical Limpet Mine used in South Africa conflicts

Similar news headlines circa 1980s

- The Star reports that a Ciskei policeman was seriously injured when a limpet mine exploded at his Mdantsane home. Police later
- Two limpet mines explode in Hillbrow
- A limpet-mine explosion kills a man outside a crowded centre in Northcliff, Johannesburg. Police suspect that the victim was ca
- A limpet-mine explosion injures nineteen people, two seriously, at a bus terminus in central Johannesburg.
- Methane gas explosion kills 68 mine workers

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Incident timeline

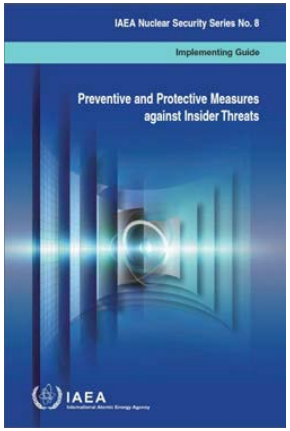
- Accidental short-circuit started a cable fire, reported in the South African press and ANC President Oliver Tambo mistakenly claimed responsibility:
  - Authorities investigated but incident was confirmed as an accident
- Wilkinson finished planting the mines on the 17th of December, setting fuses to a 24 hour delay ensuring that the plant would be deserted at the time of detonation:
  - Smuggled mines into reactor room via the ventilation system

Incident timeline

- Wilkinson then flew to Johannesburg and was taken to the Swaziland border, settled in the United Kingdom
- The mines exploded on Saturday the 18th of December over a period of several hours causing huge damage but no loss of life:
  - ANC immediately claimed responsibility for the attacks
- Wilkinson and Grey were later granted amnesty by the South African Truth and Reconciliation Commission in 1999

Insider attributes – Wilkinson

- Would you categorise him as:
  - Active vs. Passive?
  - Violent vs. non-violent?

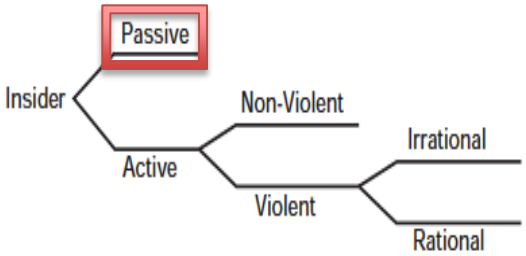


- How would you assess his level (low, medium, high) of:
  - Access?
  - Authority?
  - Knowledge?

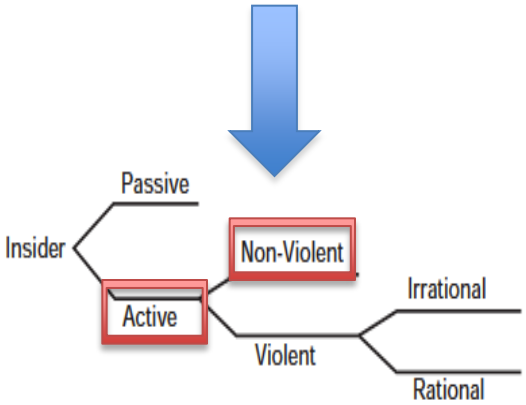
KING'S College LONDON
Los Alamos NATIONAL LABORATORY EST. 1943

Insider attributes - Wilkinson

- Access: **High**
  - Would appear he could access all the sensitive areas of the plant
- Authority: **Low**
  - But no need for the (internal) support of others
- Knowledge: **High**
  - Understood where to plant mines for maximum damage



Initial theft of information



Final sabotage attack

Security system failures

- What were the weaknesses in the security system that enabled the sabotage attack to be carried out?

Security system failures

- No comprehensive vetting system:
  - Wilkinson employed on two separate contracts with access to the most sensitive sectors of the plant but was never vetted
  - If he had been there would have identified him as a military deserter and an anti-nuclear campaigner
- Suspicious onsite behaviour unreported:
  - Gained access to the control room with a bottle of vodka (similar size to limpet mine), caught by a security guard and detained but let go with a warning

Security system failures

- Weak access control systems:
  - He was able to pass through the airlock, where he had to strip and don protective clothing, to the reactors without detection by pushing the limpet mines through an adjacent diaphragm pump & collecting them on the other side
- Failure to act on threat assessment?:
  - Paul Semark, a senior manager at the time at Koeberg has been quoted as saying, 'We knew the ANC would not target Koeberg once nuclear fuel was there… We even pinpointed 16 December 1982, which was a public holiday, as the likely date.'

References

- David Beresford, 'Truth is a Strange Fruit: A Personal Journey Through the Apartheid War', Jacana Media (Pty) Ltd (1st July 2010)
- Mohtadi, Hamid and Antu Murshid (2006), 'A Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005', p. 17, (7th July 2006)
- 'Koeberg Power Station Amnesty Decision', Department of Justice and Constitutional Development, South Africa http://www.justice.gov.za/trc/media/pr/1999/p990531b.htm (31st May 1999)
- 'How we blew up Koeberg (… and escaped on a bicycle)', Mail and Guardian, http://mg.co.za/article/1995-12-15-how-we-blew-up-koeberg-and-escaped-on-a-bicycle, (15th December 1995)
- 'Nuclear Power in South Africa', World Nuclear Association (WNA), http://www.world-nuclear.org/info/Country-Profiles/Countries-O-S/South-Africa/#.UiMd7bxOkXx (August 2013)
- "South African who attacked a nuclear plant is a hero to his government and fellow citizens", http://www.publicintegrity.org/2015/03/17/16895/south-african-who-attacked-nuclear-plant-hero-his-government-and-fellow-citizens, March 2015

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Insider Threat Case Study:

Illegal Export of ^{192}Ir from Mayak Production Association

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Methodology

- This case study was derived entirely from open sources including peer-reviewed academic articles and news reports

- The information obtained was consistent across all accounts

Overview

- Facility: Radioisotope Factory No. 45, Mayak Production Association, Russia.
- Date: August 1994 to 1997
- Incident: Illegal export of iridium-192 to the UK via falsified customs documents
- Perpetrator: Mr. A. Kalinovsky, Director of Radioisotope Factory No. 45
- Impact: Export of ^{192}Ir without a valid export license; in theory a similar method could have been used to ship sensitive nuclear material e.g. HEU

Incident timeline

- Beginning in August, 1994 Mr. A. Kalinovsky, Director of Radioisotope Factory No. 45 at the Mayak Production Association in Russia, ordered his staff to falsify customs documentation to disguise ^{192}Ir as a different isotope:
  - At the time Factory No. 45 didn't have an export license for ^{192}Ir
- The ^{192}Ir was subsequently shipped to a UK company
- In May 1995 Kalinovsky again asked his staff to falsify the documents on a shipment of ^{192}Ir, due to Factory No. 45 having already fulfilled its allowed quota under its export license:
  - Radiation levels on the shipping documentation were falsified to mask the additional ^{192}Ir

Incident timeline

- However, this time the shipment was processed at the Pulkovskiy Customs Post in St. Petersburg as opposed to a local office:
  - The experienced customs officials in St. Petersburg noticed the discrepancy between the stated and actual radiation levels
  - In response Kalinovsky ordered his staff to bring new counterfeit documents to St. Petersburg to try and move the shipment through customs
- Charges were brought against Kalinovsky for violation of customs law

Incident timeline

- However, even after Kalinovsky was charged it is reportedly that he again exported iridium to the UK by falsifying customs documentation, labeling it as cobalt:
  - This time he made sure to send the shipments through the local customs post.
- Kalinovsky appeared before court in 1997 charged with illegal exports:
  - He only received 6 years probation, even though he was found guilty
  - The prosecutor asked for a harsher sentence, but the court instead reduced the sentence to 4 years probation.

Profile - Kalinovsky

- Used his senior position at the factory to coerce workers to participate in his illicit export scheme:
  - Demonstrated the ease with which sensitive nuclear and radiological materials could be diverted by a senior insider

Security system failures

- Poor trained customs officials:
  - Unable to detect falsified shipments
- The facility appeared to lack a mechanism through which employees could question and report the actions of senior staff
- Ineffective punishment => no deterrence:
  - Kalinovsky encouraged the falsification of documents even after being charged with violating customs law
  - Eventually convicted and given just 4 years probation

Major sources

- Laurizio Martellini and Kathryn McLaughlin, 'The Security of High-Activity Radiological Sources,' Background Paper 3 for the Conference on Strengthening European Action on WMD, Non-proliferation and Disarmament (2005)
- Emily S. Ewell, ' NIS Nuclear Smuggling Since 1995: A Lull in Significant Cases?' *The Nonproliferation Review (1998)*
- Viktor Riskin, 'Mechenyye Izotopy', Chelyabinskiy Rabochiy, p. 2, (accessed via Nuclear Threat Initiative http://www.nti.org/analysis/articles/mechenyye-izotopy/) (16 June 1997)

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Insider Threat Case Study:

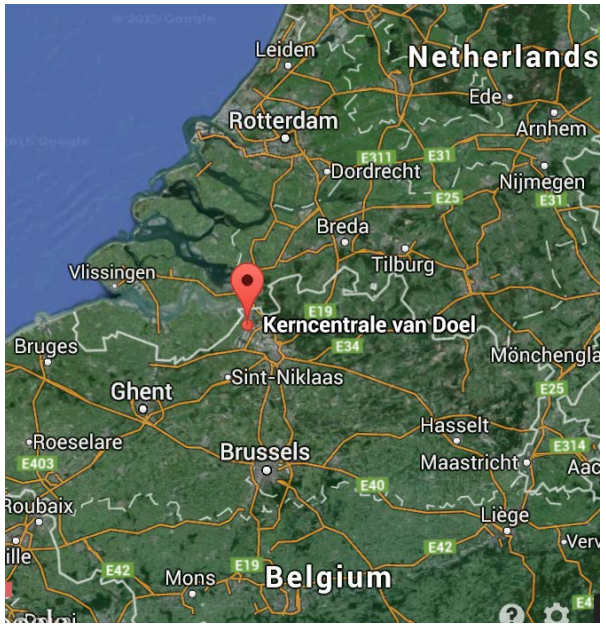
Sabotage of Doel 4 Nuclear Power Plant, Belgium

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Overview

- **Facility:** Doel 4 nuclear power plant, Belgium, operated by Electrabel GDF Suez
- **Date:** 5th August 2014
- **Incident:** Sabotage attack on reactor turbine (non-nuclear side of NPP)
- **Perpetrator:** Insider, identification unknown
- **Impact:** early estimates of financial impact of €200M, in repair to damaged turbine, loss of income, and restart; potential energy crises



KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

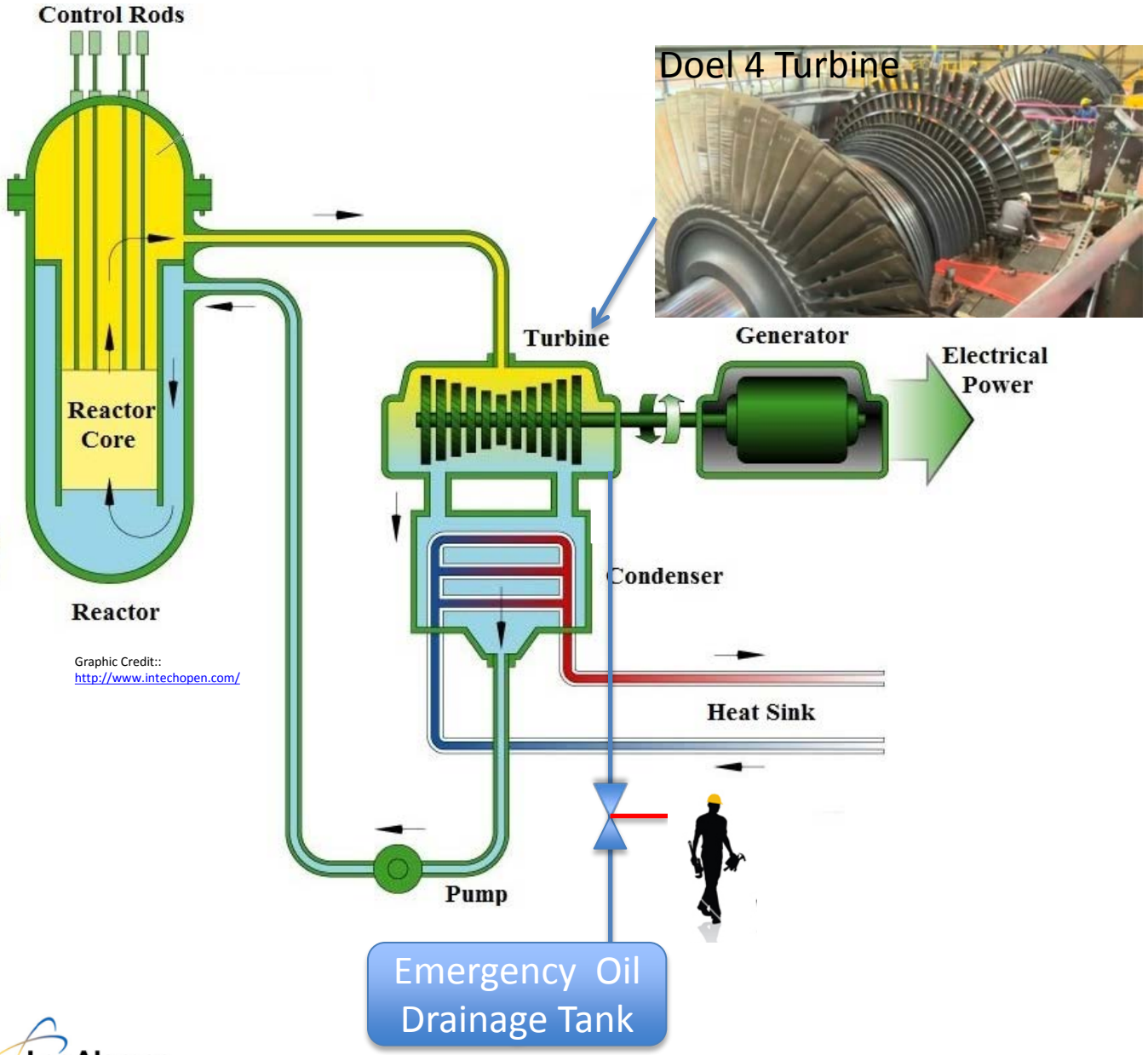
Incident timeline

- August 5, 2014: Official timeline pending
  - Morning - Doel 4 turbine operating normally at 1500 RPMs
  - Mid-day - Workers notice increase in temperature of lubricating oil in turbine in nun-nuclear side of at Doel 4 NPP
  - Workers search for cause of temperature increase, including inspection of emergency oil drain line and find emergency fire valve is in normal, closed position
  - 37 minutes from start of incident, 65,000 liters of lubricating oil drains from turbine. Turbine grinds to an abrupt stop with severe damage to the rotor blades and shaft

Incident timelines

- Subsequent investigation:
  - Workers discover that emergency oil drain valve had been intentionally opened and the act concealed
  - Valve had been secured using padlock, which was missing
  - Valve had been opened, its handle removed and re-attached to simulate closed position

Generic Power Reactor Schematic

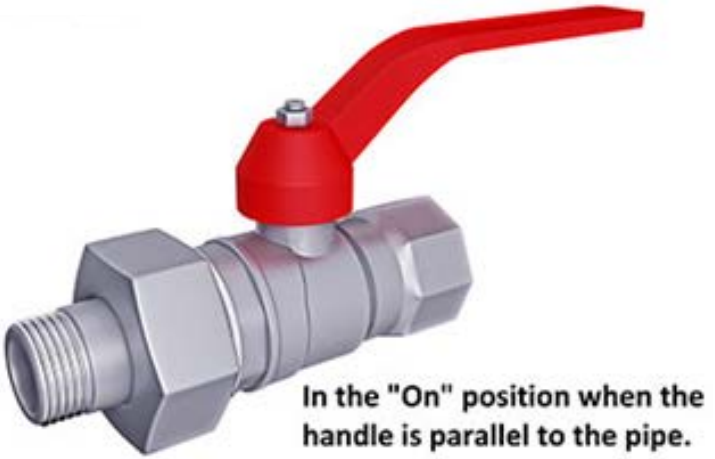


Graphic Credit::
http://www.intechopen.com/

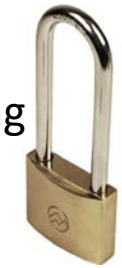
KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

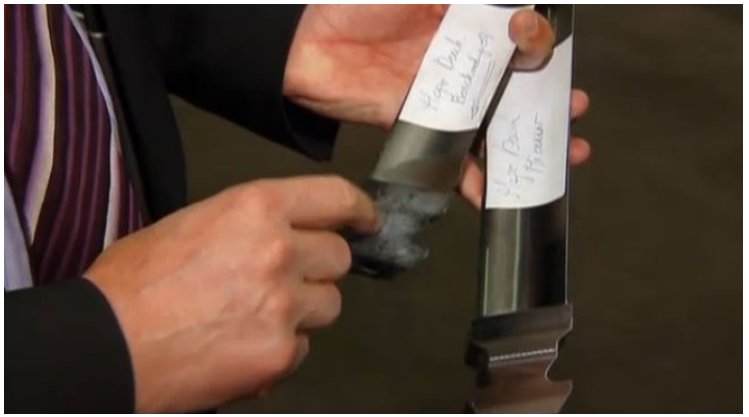
Typical Valve and Handle



Padlock was missing



Damage to the Turbine



KING'S College LONDON

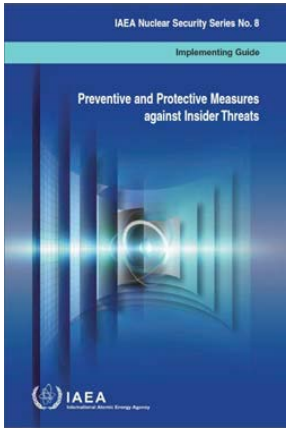
Los Alamos NATIONAL LABORATORY EST. 1943

Incident Summary

- Preliminary theory:
  - Intentional act of sabotage by an insider
  - One person, 5 minutes, €200M
- GDF Suez spokesperson was quoted "..no outsiders had penetrated into the plant.."
- Additional details of the incident have not been disclosed due to ongoing criminal investigation
- Reactor back online December 19, 2014
- No suspects publicly identified

Insider attributes – Doel 4

- Would you categorise him as:
  - Active vs. Passive?
  - Violent vs. non-violent?



- How would you assess his level (low, medium, high) of:
  - Access?
  - Authority?
  - Knowledge?

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Subgroup Exercise

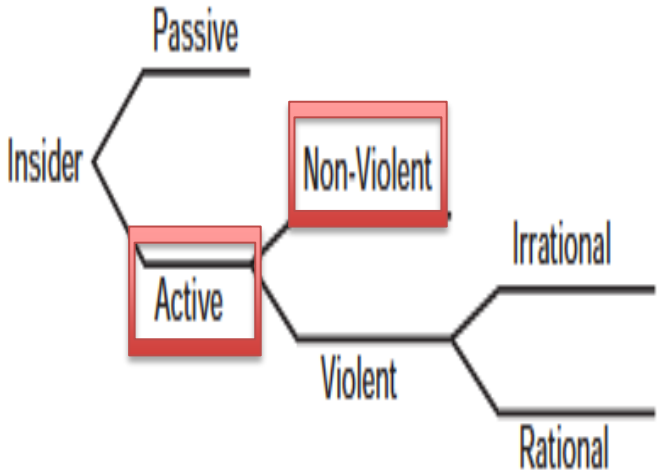
What were the security system failures?

What do you know about this insider?

How would you classify his insider attributes (Access, Authority, and Knowledge)

Insider attributes

- Access: **High**
  - Access to sensitive areas of the turbine
- Authority: **Unknown**
  - But no need for the (internal) support of others
- Knowledge: **Medium - High**
  - Understood how to cause severe damage



KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Security system failures

- One worker allowed access to sensitive equipment
- Access Control
- Able to defeat security locks

Possible Facts about this Insider

- Access to sensitive areas – probably an employee
- Understood weakness of the safety system
- Knew how to conceal the valve handle
- Must have carried at least one tool
- Had access to the key for the lock
- Kew how to escape to go unnoticed

Safety and Security Upgrades

"Recently operator Electrabel announced that the damage to the steam turbine is almost fully recovered and that a restart of the plant prepares.

In the meantime, the FANC has studied what additional measures necessary for safe and restart about talks were held with Electrabel.

The measures that will be imposed by the FANC implemented in all Belgian nuclear power plants…

Specifically, the security will be enhanced by the placement of a large number of additional cameras, through changes to the badge system, and the introduction of a series of other security measures. Also assessed was the so-called four eyes principle optimized.

In addition, the FANC also demands additional safety measures, such as additional checks on the correct configuration of the safety equipment and emergency systems."

- Statement from Agence Fédérale de Contrôle Nucléaire
Translated from Dutch:
http://www.fanc.fgov.be/nl/news/redemarrage-de-doel-4-l-afcn-impose-des-mesures-de-surete-et-de-securite-complementaires-a-toutes-les-centrales-nucleaires-belges/727.aspx

References

- "Doel 4 werkt wellicht opnieuw op 31 december", video news report, http://deredactie.be/cm/vrtnieuws/binnenland/1.2168358, 3rd December 2014

- http://deredactie.be/cm/vrtnieuws/binnenland/1.2168358
- "Enquiry into Doel 4 sabotage centres on terrorism", http://deredactie.be/cm/vrtnieuws.english/News/1.2173593, 12 December 2014

- "Electrabel confirms Doel 4 nuclear power plant sabotage", http://www.powerengineeringint.com/articles/2014/08/electrabel-confirms-doel-4-nuclear-power-plant-sabotage.html, 15 August 2014

- "Restart Goal 4: FANC imposes additional safety and security measures at all Belgian nuclear power plants", http://www.fanc.fgov.be/nl/news/heropstart-doel-4-fanc-legt-bijkomende-veiligheids-en-beveiligingsmaatregelen-op-aan-alle-belgische-kerncentrales/727.aspx, Federal

- http://nuclear-news.net/2014/08/16/sabotage-of-a-nuclear-reactor/

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Gold Theft at Los Alamos

Dr Christopher Hobbs,
King's College London,
United Kingdom

Mr Noah G Pope,
Los Alamos National Laboratory, USA

Methodology

- This case study was derived entirely from open sources including news reports, press releases, governmental reports, and peer-reviewed academic articles

- The various accounts were very consistent

Overview

- Facility: Los Alamos Plutonium Facility (PF-4) in Technical Area 55, Los Alamos, United States
- Date: March 2009
- Incident: Attempted theft of gold (contaminated with plutonium), worth an estimated $2,000
- Perpetrator: Alex Maestas – a technician at Los Alamos
- Impact: The theft was detected before the gold left PF-4

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Incident timeline

- On the 24th March 2009 Maestas was attempting to leave PF-4 when he set of a radiation portal monitor (PCM–2), a beta and gamma detector:
  - This was identified as a 50 gram piece of gold contaminated with plutonium concealed within a plastic bag
  - According to a fellow Los Alamos employee Maestas appeared surprised when PCM-2 was activated as he had scanned the gold with a hand-held alpha detector before leaving his work station
- Maestas attempted to explain his actions by claiming he was transferring the gold to a nearby machine shop:
  - However, this was deemed implausible as radioactive materials were not allowed in the machine shop

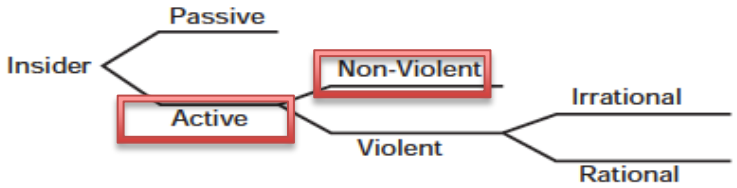
Incident timeline

- Further investigation revealed that Maestas had attempted to decontaminate the gold prior to removing it:
  - This was confirmed by Maestas who stated that 'the gold was taken from an area that was used to store materials that contained plutonium and nuclear material'
- According to the US Attorney's Office the gold posed a 'serious risk to human health', as it was contaminated with americium and plutonium and could have been deadly if inhaled:
  - Although lab officials confirmed that no one was exposed to radiation as a result of the incident
- In September 2010 he was convicted of theft and engaging in a prohibited transaction involving nuclear materials:
  - He was sentenced to one year in prison and three years of supervised release

Profile of the Perpetrator

- Maestas had worked for over 10 years (in some reports more than 20 years) as a technician at Los Alamos in a area reclaiming residual plutonium from waste materials

- He had no criminal history



KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943

Security system failures

- In this case the security system at Los Alamos functioned well with Maestas' attempt theft detected by a radiation portal monitor:
  - This was reported to be the first of eight layers of security within PF-4
- The actions of the Department of Energy personnel in apprehending Maestas and recovering the gold were praised by the US Attorney

Major sources

- 'United States v. Maestas', United States Court of Appeals, No. 10–2204, accessed via http://caselaw.findlaw.com/us-10th-circuit/1572680.html (28th June 2011)
- 'Former LANL Employee Sentenced for Stealing Irradiated Gold', FBI Albuquerque Division, http://www.fbi.gov/albuquerque/press-releases/2010/aq083110.htm (31st August 2010)
- 'Former Los Alamos lab worker accused of theft', The Seattle Times, http://seattletimes.com/html/nationworld/2010034663_apuslabtheftcharge.html?syndication=rss (9th October 2009)

KING'S College LONDON

Los Alamos NATIONAL LABORATORY EST. 1943